

RAW MATERIAL CAPTCHA SECURITY, APPLIED THROUGH ZOPFLI TECHNIQUE

P. RAJENDIRAN, K. R. SEKAR, B. SRINIVASAN & R. MANIKANDAN

School of Computing, SASTRA University, India

ABSTRACT

In the manufacturing unit, production plays the important role. Requirement analysis, procuring materials from the third party vendors, quality checking towards the product and storage are the main integral segments, in the manufacturing side. The non functional activity like security is an inevitable commodity that gives a great security, to the materials procured. In the storage segments, recognized persons are allowed to access the raw materials, to make the shipment from stores to production, according to their requirements. Security can be imposed via captcha model and in this research article, the same phenomena is applied and compressed through Zopfli technique. This research brings up the greater security to the materials and the raw material handling, and wastage can be prevented to the great extent in the manufacturing industries. The compression and security technologies are applied through computer techniques.

KEYWORDS: Raw Material, Captcha Security, Data Compression & Zopfli Captcha Security

Received: Sep 25, 2017; **Accepted:** Oct 13, 2017; **Published:** Oct 31, 2017; **Paper Id:** IJMPERDDEC201710

INTRODUCTION

In the manufacturing unit, raw material shipment from store to production is the important phenomena and at the same point of time, security is also the major role. First come first serve is the principle followed in the all the manufacturing unit, in terms with stores. Ruthless handling of the materials will cause heavy loss to the manufacturing industry. Captcha security can prevent the enforcing schedule and scrap to the greater side. Optimization refers here as a less amount of materials with a greater service, through the product and make wastage reduce via security measures. Zopfli techniques applied in captcha, to reduce the space and size which refers to as optimized martial handling.

The main disturbing concern on any authentication and security mechanisms is the brute force attacks, by the bots from the system. This needs to be addressed and found a solution, in such a way that both the stopping of the brute force attacks and the simplicity of the authentication process are not compromised. Hence, we propose a new captcha mechanism- the Common sense based captcha. This captcha mechanism works beautifully in such a manner that, it basically tests the common sense of a human being, which any bot will completely lag. Then, in our second part of our paper, we are proposing a novel mechanism, to efficiently use the Zopfli compression mechanism [5], in such a way that, it greatly reduces the size of the file that needs to be transferred over the net. These we see in detail, in the following sections.

LITERATURE SURVEY

There are several current image based captcha authentication mechanisms. A careful study of these present

types and different forms of image based authentication captcha mechanisms, reveal several disadvantages in each of the image based authentication mechanism. A few of them produce images that are having a noise ratio at a higher rate, which makes it easier for Signal propagation attack, to be easily carried upon them. Several other images have a lesser number of image pool that are available, which makes them vulnerable to mechanical turk attacks and challenge replay attacks [4]. A few of the text based captcha that is used by different famous websites are listed below, in the figure.

Table 1: Text Based Captcha used in Various Websites

Sr. No.	Text based CAPTCHA	Website
1		Wikipedia[6]
2		Yahoo[7]
3		Microsoft[8]
4		Mailblocks[9]
5		Ticket Master[10]
6		Alta Vista [11]
7		Facebook [12]

On the second part of the paper, there are several compression techniques that are being used, as of today. The most famous ones are the gzip, kzip, zlib and the zopfli. The main objectives of these types of compression are that, they need to reduce the payload size of the webpage that, they are used in. When these compression algorithms are used in such a manner, they have to be made certain that, they do not eat up CPU cycles. So, a compromise on the bandwidth is taken. As of today, most of these types of compression are used, in compressing webpage on demand. But, these compression algorithms can also be used, to compress files that need to be sent over the internet. Especially, for the files which are of static nature, where we can use this in a manner such as, to compress once and transfer multiple times. So, among all of these compression algorithms, Zopfli algorithm is chosen. This is because that, zopfli algorithm produces the highest possible density, in compressing the files comparing to others.

EXISTING METHODS AND DRAWBACKS

Captcha

Existing Methods

There are several existing captcha mechanisms that are available, as of today. Few of them include captcha, using image [1] numbers and text, puzzle solving etc. Facebook.com captcha system and reCAPTCHA are just a few examples for the case in point. The facebook.com captcha system gives the captcha to the users in such a way that, two dictionary phrases are placed side by side, into a single captcha. In the other example, [2]reCAPTCHA, an OCR work unit is presented, along with a text and presented as a captcha. These are some of the several captcha mechanisms that are being in

use, as of today.

Drawbacks

There are several drawbacks to the existing Captcha mechanisms. The drawbacks can be broadly classified into two important factors. The first concerning the security of the Captcha that is being used [3] and the second is concerning the User convenience, for the persons using the captcha. When one is given prime importance, the other factor invariably reduces. Thus, an optimum needs to be found in such a way that it provides a better security and also makes the user convenience, much simpler and elegant. The present existing captcha mechanisms [4] are vulnerable to different types of attacks. Some of the common types of attacks are:

- Bypass Attacks
- Challenge Replay Attacks
- Signal Processing Attacks, etc.

With these types of attacks that are actively existing and being tried upon on captcha mechanisms, the invariable need for improving the security increases.

COMPRESSION

Existing Methods

There are several compression techniques that are available and are being used, in today's world. Few of the famous compression techniques that are widely used are gzip, kzip, 7-zip, bicriteria data compression [5] etc. The most commonly used compression technique among these is the gzip [6] compression. This is because of the availability of the huge number of documentations for it.

Drawbacks

The main drawback in using these types of compression are that, when saving bandwidth becomes the core criteria, compromising on the load of the server or on the system, the amount of compression attains the premier role. The more the files that needs to be sent are compressed, the better it will be for the clients receiving it, at the user end. Thus, there is a better need for the compression techniques to perform in such a way that, the ratio of compression size is higher.

PROPOSED SOLUTION AND ADVANTAGES

Captcha

To eliminate brute force attacks from bots and to authenticate an actual user, a new type of captcha mechanism is proposed in this paper. This uses the image based captcha authentication technique, which will be much simpler for the users and much difficult for the bots, to crack through. This is because of the fact that, the image based authentication makes a common sense test to the user, which only a human will be able to succeed.

This captcha mechanism is basically placed in such a manner, where the users will feel the level of ease, while they use this. In this, the users accessing a particular site will be challenged, with a set of names of photos that are to be displayed below. The users then have to study the question that is thrown at them, perceive and interpret them and give their response. Their response will be designed in such a simple way that, the users will just have to click on the above

challenged images, in their correct order.

If the users fail to click on the correct image, or if the users fail to click the images in their respective given order of the question, then at that particular instance, the captcha will be invalid. The users will have to retake the captcha test again and succeed, in order to proceed further.

Advantages

The main advantage of using this type of captcha authentication mechanism is that, this image based authentication mechanism holds strong against bypass attacks and signal processing attacks. When this is combined with a simple common sense testing, the factor of security increases to a much higher rate. As a result, this will also hold strong against attacks, such as challenge replay attacks, brute force attacks or even against hybrid attacks.

This captcha remains at the top for the user simplicity because, this basically uses only the GUI representation and does not ask or challenge the users, using the captcha to take the trouble in typing the respected captcha, from the challenged image or text.

COMPRESSION

The proposed method is that of using the existing Zopfli compression, into compressing the corpora or any form of file that needs to be transferred over the internet, before they are being uploaded into the server to send it. Performing this compression, using the Zopfli compression greatly advances the level and the amount of the compression that is done, compared to the other compression techniques [5]. The Zopfli is designed in such a manner that, it is compatible with deflate. This facilitates the use of the zopfli compression because, any web browser that is compatible with deflate will be able to decompress the files, that are compressed using zopfli. The zopfli basically works on modeling of the entropy and their iteration, and by finding a shortest path to the graph of the deflate representation.

Advantage Issues

The main advantage of using the Zopfli [6] compression is that, it reduces and saves the usage of the bandwidth, by compressing the files at a very higher rate, when compared to other compression algorithms. This not only saves the bandwidth, but also reduces the battery consumption in mobile, as the page load will be lesser and will be able to load at a faster rate. This technique is best suited, where a same file is sent over the internet several times, that is, any static data content over the webpage.

RESULTS AND DISCUSSIONS

Captcha

The main functionality of any captcha mechanism is that, the captcha must hold well against many types of attacks that are levied, on the captcha system. The image based authentication technique for the captcha, will strongly hold against several attacks such as bypass attacks, signal propagation attacks, brute force attacks, challenge replay attacks, hybrid attacks, etc.

The reason that, the proposed captcha technique will hold good against this number of attacks is mainly, because of the number of permutations and combinations of the images that are possible to display in the captcha, from the total pool of a number of images available. For instance, if the total number of images that are available in the image pool is taken as n , then the total number of possibilities of permutation and combination can be given through this,

$${}_nP_r$$

Where, P is the total permutation possible and r is the required number of images at a single captcha. This total permutation is just for the images. When the permutation for the challenge questions are also taken into account, their odd increases by many a factor. Despite all these sophistication and security, the user simplicity still remains at a very simple form, compared to other captcha mechanisms.

Compression

The compression of any files that needs transferred can be done, using zopfli. This is because, on comparison, it is noticed that, the compression done using the zopfli give a higher compression ratio of up to 5%, more than that of the other similar compression techniques. One main disadvantage in using the zopfli is that, the compression time is at a higher note, when compared to the other compression techniques. But, this is to overcome in its decompressing time, which is faster than the others of its league. In order to keep the CPU usage cycle to its minimum, this Zopfli compression could be used for compressing and sending files of static nature.

A comparative study of all the compression algorithms is found in a study, which is analyzed and given briefly in the following table.

Table 2: Comparison of Different Compression Technique

Factors	Gzip	7-Zip	Kzip	Zopfli
Compression Size	36,445,248 bytes	35,102,976 bytes	35,025,767 bytes	34,995,756 bytes
Compression Time	5.60s	128s	366s	454s
Decompression Time	934ms	949ms	937ms	926ms

CONCLUSIONS

In the manufacturing and the production unit literally needs heavy protocols to be followed, so as to prevent unwanted wastages. The wastage reduction brings more mileage and milestone to the high level products. The optimization principles provide greater vision, in utilizing raw materials in the production side. The manufacturing units needs to gain high profit so that, to get a greater shares from the public. The Captcha security avoids wastages, because of handling products in a right manner. Now a day, all the manufacturing industries look for the security, for handling products and raw materials. The techniques like Zopfli compression provide high security level, in handling products to the core. For future development on this, the image based captcha mechanism can be further improved by developing this technique in generating a one-time password (OTP), or can also be developed in making a better common sense test to the users. In the compression side, an analysis of a best compression technique that can be used, for each and every particular data can be studied and implemented in the manufacturing segment.

REFERENCES

1. Doyle Ryan, *Image-based CAPTCHA with JACI*, Box Hill Institute, Centre for ICT.]
2. Chew, Monica and Tygar, J. D., *Image Recognition CAPTCHAs*, 7th International Information Security Conference (ISC 2004), Springer, pp. 268-279, September 2004.
3. Lorenzi, David et al, *Attacking Image Based CAPTCHAs Using Image Recognition Techniques*, 8th International Conference, ICISS 2012, Springer, pp. 327-342, 2012

4. *Azad, Silky and Jain, Kiran, CAPTCHA: Attacks and Weaknesses against OCR Technology, Global Journals Inc, Volume 13 Issue 3, 2013*
5. *Alakuijala Jyrki, Vandevenne Lode, Data compression using Zopfli, Google Inc.*
6. *Farruggia, Andrea et al, Bicriteria data compression, Dipartimento di Informatica, Universit a di Pisa, Italy.*